

# Zależności między liczbami Strlinga pierwszego i drugiego rodzaju

Zauważmy, że liczba cykli musi być co najmniej równa liczbie podzbiorów, więc mamy

$$\left\{ \begin{matrix} n \\ k \end{matrix} \right\} \leq \left[ \begin{matrix} n \\ k \end{matrix} \right]$$

dla całkowitych nieujemnych  $n$  i  $k$ .

Zachodzą tzw. wzory *inwersji*:

Jeżeli  $m \neq n$ , to

$$\sum_{k=m}^n \left[ \begin{matrix} n \\ k \end{matrix} \right] \left\{ \begin{matrix} k \\ m \end{matrix} \right\} (-1)^{n-k} = \sum_{k=m}^n \left\{ \begin{matrix} n \\ k \end{matrix} \right\} \left[ \begin{matrix} k \\ m \end{matrix} \right] (-1)^{n-k} = 0$$

Wartości  $\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$  dla małych  $n$  i  $k$ :

$n \backslash k$	0	1	2	3	4	5	6	7	8	9
0	1	0	0	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0	0	0	0
2	0	1	1	0	0	0	0	0	0	0
3	0	1	3	1	0	0	0	0	0	0
4	0	1	7	6	1	0	0	0	0	0
5	0	1	15	25	10	1	0	0	0	0
6	0	1	31	90	65	15	1	0	0	0
7	0	1	63	301	350	140	21	1	0	0
8	0	1	127	966	1701	1050	266	28	1	0
9	0	1	255	3025	7770	6951	2646	462	36	1

**Uwaga!**

W przypadku, gdy  $n \geq 0$  i  $k < 0$  zakładamy, że  $\left\{ \begin{matrix} n \\ k \end{matrix} \right\} = 0$ .

## Przykład

Oblicz wartości wyrażeń

a)  $x^1 + x^2$ ,

b)  $x^1 + 3x^2 + x^3$ ,

c)  $x^1 + 7x^2 + 6x^3 + x^4$ .

d)  $x^1 + 15x^2 + 25x^3 + 10x^4 + x^5$ .

Powyższy przykład pokazuje, że dla małych wartości  $n$  wyrażenie  $x^n$  można zapisać jako sumę potęg zstępujących ze współczynnikami wynikającymi z tabeli liczb Stirlinga drugiego rodzaju:

$$x^0 = x^0,$$

$$x^1 = x^1,$$

$$x^2 = x^1 + x^2,$$

$$x^3 = x^1 + 3x^2 + x^3,$$

$$x^4 = x^1 + 7x^2 + 6x^3 + x^4,$$

$$x^5 = x^1 + 15x^2 + 25x^3 + 10x^4 + x^5.$$

Czy prawdziwa jest ogólna zależność?

Wartości  $\begin{bmatrix} n \\ k \end{bmatrix}$  dla małych  $n$  i  $k$ :

$n \backslash k$	0	1	2	3	4	5	6	7	8
0	1	0	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0	0	0
2	0	1	1	0	0	0	0	0	0
3	0	2	3	1	0	0	0	0	0
4	0	6	11	6	1	0	0	0	0
5	0	24	50	35	10	1	0	0	0
6	0	120	274	225	85	15	1	0	0
7	0	720	1764	1624	735	175	21	1	0
8	0	5040	13 068	13 132	6769	1960	322	28	1
9	0	40 320	109 584	118 124	67 284	22 449	4536	546	36

**Uwaga!**

W przypadku, gdy  $n \geq 0$  i  $k < 0$  zakładamy, że  $\begin{bmatrix} n \\ k \end{bmatrix} = 0$ .

## Przykład

- $5^{\underline{3}} = 5 \cdot 4 \cdot 3 = 60$
- $5^{\overline{3}} = 5 \cdot 6 \cdot 7 = 210$
- $4^{\underline{5}} = 4 \cdot 3 \cdot 2 \cdot 1 \cdot 0 = 0$

$$n! = n^{\underline{n}} = 1^{\overline{n}}$$

## Przykład

- $x^{\underline{3}} = x(x-1)(x-2) = x^3 - 3x^2 + 2x$
- $x^{\overline{3}} = x(x+1)(x+2) = x^3 + 3x^2 + 2x$

## Przykład

Zapisz w postaci ogólnej wielomiany  $x^{\overline{s}}$  dla  $s = 0, 1, 2, 3, 4, 5$ .

$$x^{\overline{0}} = 1 = x^0,$$

$$x^{\overline{1}} = x = x^1,$$

$$x^{\overline{2}} = x(x+1) = x^1 + x^2,$$

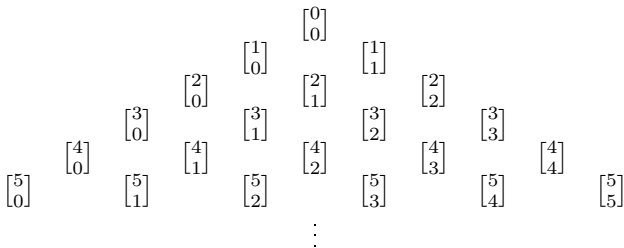
$$x^{\overline{3}} = x(x+1)(x+2) = 2x^1 + 3x^2 + x^3,$$

$$x^{\overline{4}} = x(x+1)(x+2)(x+3) = 6x^1 + 11x^2 + 6x^3 + x^4,$$

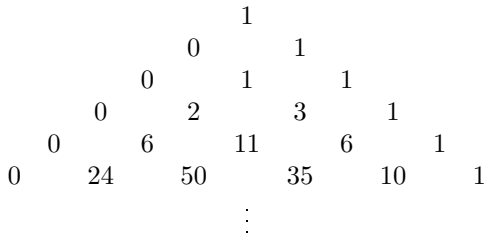
$$x^{\overline{5}} = x(x+1)(x+2)(x+3)(x+4) = 24x^1 + 50x^2 + 35x^3 + 10x^4 + x^5.$$

Jak powinno wyglądać uogólnienie zaobserwowanych wyników?

### Trójkąt Stirlinga dla cykli:



### Trójkąt Stirlinga dla cykli:



## Dowód. (2/2)

W drugim przypadku mamy  $\begin{bmatrix} n-1 \\ k \end{bmatrix}$  możliwości podziału zbioru  $\{a_1, a_2, \dots, a_{k-1}\}$  na cykle  $C_1, C_2, \dots, C_k$ . W przypadku każdego takiego podziału element  $a_n$  może trafić do jednego z tych cykli. Nietrudno zauważyć, że można go tak umieścić na  $(n-1)$  sposobów (cykl długości  $L$  można rozszerzyć o jeden element na  $L$  sposobów). Zatem w tym przypadku mamy  $(n-1) \cdot \begin{bmatrix} n-1 \\ k \end{bmatrix}$  możliwości.

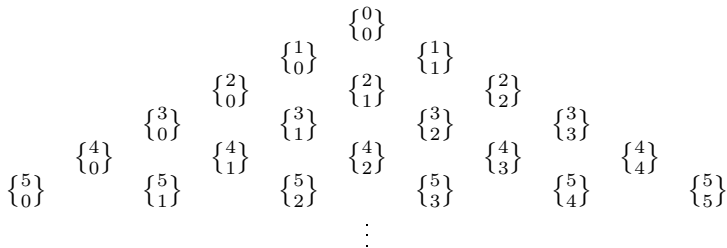
Ostatecznie

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + (n-1) \cdot \begin{bmatrix} n-1 \\ k \end{bmatrix}.$$

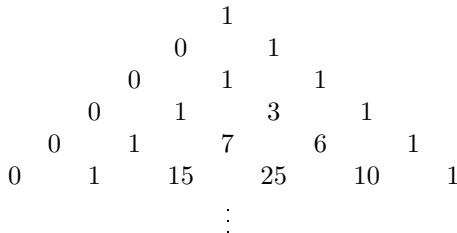




Trójkąt Stirlinga dla podzbiorów:



Trójkąt Stirlinga dla podzbiorów:



## Twierdzenie

Dla  $n > 0$  zachodzi zależność rekurencyjna

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + (n-1) \cdot \begin{bmatrix} n-1 \\ k \end{bmatrix}.$$

Poniższy dowód jest modyfikacją wcześniej przedstawionego dowodu zależności rekurencyjnej dla liczb Stirlinga drugiego rodzaju.

## Dowód. (1/2)

Niech  $S = \{a_1, a_2, \dots, a_n\}$ . Określimy liczbę podziałów  $S$  na  $k$  cykli  $C_1, C_2, \dots, C_k$ . Zauważmy, że w każdym takim podziale elementy  $a_1, a_2, \dots, a_{n-1}$  można rozmieścić albo w cyklach  $C_1, C_2, \dots, C_{k-1}$  albo w cyklach  $C_1, C_2, \dots, C_{k-1}, C_k$ .

W pierwszym przypadku mamy  $\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}$  możliwości. Zauważmy, że dla każdego takiego podziału element  $a_n$  tworzy ostatni, jednoelementowy cykl  $C_k = [a_n]$ .

## Przykład

Wyznaczyć największy wspólny dzielnik oraz najmniejszą wspólną wielokrotność liczb 48 i 180.

Stosując algorytm Euklidesa otrzymujemy

$$180 = 3 \cdot 48 + 36$$

$$48 = 1 \cdot 36 + 12$$

$$36 = 3 \cdot 12$$

Zatem  $\text{NWD}(48, 180) = 12$ .

Z faktu  $\text{NWD}(a, b) \cdot \text{NWW}(a, b) = |a \cdot b|$  otrzymujemy  $\text{NWW}(a, b) = \frac{|a \cdot b|}{\text{NWD}(a, b)}$ .

Zatem

$$\text{NWW}(48, 180) = \frac{48 \cdot 180}{12} = \frac{4 \cdot 180}{1} = 720.$$

## Podstawowe twierdzenie arytmetyki

Każdą liczbę całkowitą dodatnią można przedstawić jako iloczyn liczb pierwszych. Przedstawienie takie jest jednoznaczne z dokładnością do kolejności czynników.

### Przykład

$$12 = 2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2$$

## Wniosek

Każda większa od 1 liczba naturalna  $n$  może być jednoznacznie zapisana w tzw. **postaci kanonicznej**

$$n = q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdot \dots \cdot q_k^{\alpha_k},$$

gdzie  $q_i$  są liczbami pierwszymi,  $\alpha_i$  są liczbami naturalnymi oraz  $q_1 < q_2 < \dots < q_k$ .

### Przykład

Postacią kanoniczną liczby 12 jest  $2^2 \cdot 3$ .

## Definicja

Dla każdej liczby  $n \in \mathbb{N}/\{1\}$  określamy liczbę  $\varphi(n)$  jako liczbę dodatnich liczb całkowitych mniejszych od  $n$  i względnie pierwszych z  $n$ :

$$\varphi(n) = \left| \{1 \leq k < n : k \perp n\} \right|.$$

Funkcję  $\varphi = \varphi(n)$  nazywamy **funkcją  $\varphi$ -Eulera**.

## Przykład

Obliczmy  $\text{NWD}(k, 12)$  dla  $k$  mniejszych od 12:

$$\begin{array}{llll} \text{NWD}(1, 12) = 1, & \text{NWD}(4, 12) = 4, & \text{NWD}(7, 12) = 1, & \text{NWD}(10, 12) = 2, \\ \text{NWD}(2, 12) = 2, & \text{NWD}(5, 12) = 1, & \text{NWD}(8, 12) = 4, & \text{NWD}(11, 12) = 1. \\ \text{NWD}(3, 12) = 3, & \text{NWD}(6, 12) = 6, & \text{NWD}(9, 12) = 3, & \end{array}$$

Zatem

$$\varphi(12) = \left| \{1, 5, 7, 11\} \right| = 4.$$

## Poprawność algorytmu Euklidesa

- Algorytm produkuje malejący ciąg liczb całkowitych nieujemnych  $r_1 > r_2 > \dots > r_n$  (jedna liczba w jednym kroku). Zatem algorytm zatrzymuje się po skończonej liczbie kroków (nie większej niż wartość  $r_1$ ).
- Z własności  $\text{NWD}(a, b) = \text{NWD}(a - qb, b)$  otrzymujemy

$$\begin{aligned}\text{NWD}(a, b) &= \text{NWD}(b, r_1) = \text{NWD}(r_1, r_2) = \dots = \text{NWD}(r_{n-1}, r_n) = \\ &= \text{NWD}(r_n, 0) = r_n\end{aligned}$$

## Twierdzenie

Liczb pierwszych jest nieskończenie wiele.

## Dowód.

Żałóżmy nie wprost, że teza twierdzenia jest fałszywa, tj. zbiór liczb pierwszych jest skończony. Zatem dla pewnej liczby naturalnej  $n$  mamy

$$\mathbb{P} = \{p_1, p_2, \dots, p_n\}.$$

Niech  $P$  będzie następnikiem iloczynu wszystkich elementów powyższego zbioru  $\mathbb{P}$ :

$$P = 1 + \prod_{i=1}^n p_i.$$

Zauważmy, że liczba  $P$  przy dzieleniu przez  $p_i$  (dla  $i = 1, 2, \dots, n$ ) daje resztę 1, zatem liczba  $P$  nie jest podzielna przez żadną liczbę pierwszą — uzyskaliśmy sprzeczność. □

Powyższy dowód ma  $\sim 2500$  lat (*Elementy* Euklidesa).

## Definicja

Liczba  $n \in \mathbb{N}$  jest **liczbą pierwszą**, jeżeli  $n$  ma dokładnie dwa dodatnie dzielniki.

- 0 nie jest liczbą pierwszą (po pierwsze nie jest liczbą dodatnią, a po drugie ma nieskończenie wiele dzielników).
- 1 nie jest liczbą pierwszą (ma dokładnie jeden dodatni dzielnik).
- Początkowe liczby pierwsze: 2, 3, 5, 7, 11, 13, 17, 19, 23.
- Liczby naturalne większe od 1 dzielimy na liczby pierwsze i liczby złożone (złożone to te, które nie są pierwsze).
- 1 nie jest ani liczbą pierwszą, ani liczbą złożoną.
- Zbiór liczb pierwszych oznaczamy przez  $\mathbb{P}$ .



## Twierdzenie (NWD jako kombinacja liniowa)

Dla  $a, b \in \mathbb{Z}$  takich, że co najmniej jedna z nich jest różna od 0, istnieją  $u, v \in \mathbb{Z}$  takie, że

$$\text{NWD}(a, b) = u \cdot a + v \cdot b.$$

Ponadto  $\text{NWD}(a, b)$  jest najmniejszą możliwą dodatnią kombinacją liniową  $a$  i  $b$ .

## Przykład

Wyznaczyć najmniejszą dodatnią kombinację liniową liczb 3 i 7 oraz podać jej przykładowe współczynniki.

$$\text{NWD}(3, 7) = 1 = 5 \cdot 3 - 2 \cdot 7$$

$$1 = (-2) \cdot 3 + 1 \cdot 7$$

$$1 = (-23) \cdot 3 + 10 \cdot 7$$

$ x $	wartość bezwzględna liczby $x$
$\text{NWD}(a, b)$	największy wspólny dzielnik liczb $a$ i $b$
$\text{NWW}(a, b)$	najmniejsza wspólna wielokrotność liczb $a$ i $b$
$\min\{a, b\}$	niewiększa z liczb $a$ i $b$
$\max\{a, b\}$	niemniejsza z liczb $a$ i $b$
$a b$	liczba $a$ jest dzielnikiem liczby $b$
$a \perp b$	liczby $a$ i $b$ są względnie pierwsze
$\mathbb{N}$	zbiór liczb naturalnych, $\mathbb{N} = \{1, 2, 3, \dots\}$
$\mathbb{Z}$	zbiór liczb całkowitych, $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
$\mathbb{Z}_n$	zbiór reszt z dzielenia przez $n$ , $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$
$\mathbb{P}$	zbiór liczb pierwszych
$p_i$	$i$ -ta liczba pierwsza

# Odwrotny algorytm Euklidesa

Algorytm służy wyznaczenia  $u$  i  $v$  takich, że  $a \cdot u + b \cdot v = \text{NWD}(a, b)$ .

- Obliczamy  $\text{NWD}(a, b)$  korzystając z algorytmu Euklidesa otrzymując ciąg równań

$$a = q_1 \cdot b + r_1, \quad b = q_2 \cdot r_1 + r_2, \quad r_1 = q_3 \cdot r_2 + r_3, \quad \dots, \\ r_{n-3} = q_{n-1} \cdot r_{n-2} + r_{n-1}, \quad r_{n-2} = q_n \cdot r_{n-1} + r_n, \quad r_{n-1} = q_{n+1} \cdot r_n.$$

- Z  $i$ -tego równania wyznaczamy wartość  $r_i$  dla każdego  $i = 1, 2, \dots, n$  (więc pomijamy ostatnie równanie).
- Wyliczone  $r_n$  daje nam równanie  $\text{NWD}(a, b) = r_{n-2} - q_n \cdot r_{n-1}$ .  
Do tego równania wstawiamy wyliczoną wartość  $r_{n-1}$  (w ten sposób otrzymujemy  $\text{NWD}(a, b)$  w kombinacji liniowej  $r_{n-2}$  i  $r_{n-3}$ ).
- Kontynuujemy podstawianie  $r_{n-2}$ ,  $r_{n-3}$  itd. aż do  $r_1$ , po drodze upraszczając współczynniki. W efekcie dostajemy zapis implikujący wartości  $u$  i  $v$ .

## Stwierdzenie

Jeżeli  $a \perp b$ , to  $\varphi(ab) = \varphi(a)\varphi(b)$ .

Z dwóch ostatnich stwierdzeń wynika następujące

## Twierdzenie

Niech  $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$  będzie postacią kanoniczną liczby  $n \in \mathbb{N}/\{1\}$ . Wtedy

$$\varphi(n) = n \cdot \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right).$$